

Handwritten mark



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/544,069	04/06/2000	Natsume Matsuzaki	NAKI-BK59	9251
21611	7590	06/17/2004	EXAMINER	
SNELL & WILMER LLP 1920 MAIN STREET SUITE 1200 IRVINE, CA 92614-7230			SMITHERS, MATTHEW	
			ART UNIT	PAPER NUMBER
			2137	2

DATE MAILED: 06/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Handwritten mark

Office Action Summary

Application No.

09/544,069

Applicant(s)

MATSUZAKI ET AL.

Examiner

Matthew B Smithers

Art Unit

2137



-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 April 2000.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☒ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

Art Unit: 2137

DETAILED ACTION

Priority

Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Japan on 07 April 1999. It is noted, however, that applicant has not filed a certified copy of the 11-099657 application as required by 35 U.S.C. 119(b).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-17 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. patent 6,026,421 granted to Sabin et al.

Regarding claim 1, Sabin meets the claimed limitations as follows:

“A multi-word arithmetic device for executing modular arithmetic on multi-word integers, in accordance with instructions from an external device, the multi-word arithmetic device comprising:

a memory; ” see Figure 1, element 12.

Art Unit: 2137

“an arithmetic unit for executing, on word units, at least two types of calculation, including addition and multiplication, and outputting a one-word calculation result;” see column 3, lines 26-33.

“a memory input/output circuit for performing (1) a first data transfer for storing in the memory at least one integer received from an external device, (2) a second data transfer for inputting at least one integer stored in the memory into the arithmetic unit in word units, (3) a third data transfer for storing in the memory the calculation result output from the arithmetic unit, and (4) a fourth data transfer for outputting the calculation result from the memory to the external device;” see column 7, line 61 to column 8, line 20 and column 12, line 40 to column 13, line 20.

“and a control circuit for, according to instructions received from the external device,

(a) specifying, to the memory input/output unit, data to be transferred by the second and third data transfers,

and (b) specifying, to the arithmetic unit, a type of calculation to be executed, thereby controlling: (i) the arithmetic unit to selectively perform one of at least two types of modular arithmetic on the at least one integer stored in the memory; and (ii) the memory input/output circuit to store the calculation result of the modular arithmetic into the memory.” see column 11, lines 42-49 and column 12, line 30 to column 13, line 20.

Regarding claim 2, Sabin meets the claimed limitations as follows:

“The multi-word arithmetic device of Claim 1, wherein at least two integers are stored in the memory, the arithmetic unit includes: an adder for adding at least two pieces of

Art Unit: 2137

one-word data; and a multiplier for multiplying at least two pieces of one-word data, and the memory input/output circuit simultaneously reads one word from each of the at least two integers stored in the memory, and outputs the read words to one of the adder and the multiplier.” see column 3, lines 26-33; column 3, lines 50-56 and column 12, line 30 to column 13, line 20.

Regarding claim 3, Sabin meets the claimed limitations as follows:

“The multi-word arithmetic device of Claim 2, wherein:

the memory is divided into two dual-port memories, each allowing access to two storage areas designated by two addresses, and allowing (1) two read operations, or (2) one read operation and one write operation to be performed simultaneously on word units; and the at least two integers are stored in each dual-port memory so that the memory input/output: circuit can simultaneously (1) read a piece of one-word data simultaneously from each of the integers stored in the two dual-port memories, and have the read pieces of data input into one of the adder and the multiplier, and (2) write a piece of one-word data output from one of the adder and the multiplier into one of the two dual-port memories.” see column 14, lines 28-53.

Regarding claim 4, Sabin meets the claimed limitations as follows:

“The multi-word arithmetic device of Claim 1, wherein the arithmetic unit, according to instructions from the control circuit, executes one of the following three calculations: (1) addition: of at least two pieces of one-word data; (2) multiplication of two pieces of one-word data; and (3) multiplication of two pieces of one-word data and accumulation

Art Unit: 2137

of multiplication results.” see column 3, lines 26-33; column 3, lines 50-56; column 7, line 33 to column 8, line 20 and column 12, line 30 to column 13, line 20.

Regarding claim 5, Sabin meets the claimed limitations as follows:

“The multi-word arithmetic device of Claim 4, wherein the arithmetic unit includes:

a multiplier receiving an input of two pieces of one-word data and outputting a piece of two-word data;

an adder receiving an input of at least two pieces of two-word data, including a piece of two-word data output from the multiplier, and outputting a piece of multi-word data; and

a selecting circuit selecting, according to instructions from the control circuit:

(1), data to be input into one of the multiplier and the adder out of data transmitted from the memory input/output circuit; and

(2) data to be output as the calculation result out of data output from one of the adder and the multiplier.” see column 3, lines 26-33; column 3, lines 50-56; column 7, line 33 to column 8, line 20 and column 12, line 30 to column 13, line 20.

Regarding claim 6, Sabin meets the claimed limitations as follows:

“The multi-word arithmetic device of Claim 1, wherein the at least two types of modular arithmetic include modular addition, and on receiving, from the external device, an instruction to execute modular addition and an indication of a number of words n for each integer on which modular addition is to be performed, the control circuit controls the memory input/output circuit and the arithmetic unit to execute the following processing:

Art Unit: 2137

the memory input/output circuit obtains from the external device and stores in the memory two n-word integers A and B on which modular addition is to be executed and a n-word integer P showing a modulus;

(2) the memory input/output circuit (a) reads simultaneously, from the integers A, B and P stored in the memory, pieces of one-word data a, b and p, each with a same digit position, and has the read pieces of data input into the arithmetic unit, while (b) storing in the memory a piece of one-word data w output from the arithmetic unit, and repeats processes (a) and (b) sequentially from a lowest-order word in each integer until n words of data are obtained, enabling an n-word integer W to be stored in the memory; and

(3) the arithmetic unit repeats n times a process in which the pieces of data a, b and p received from the memory input/output circuit are computed as $a + b - p$, propagating a carry, and a result w is output.” see column 3, lines 26-33; column 3, lines 50-56; column 7, line 33 to column 8, line 20 and column 12, line 30 to column 13, line 20.

Regarding claim 7, Sabin meets the claimed limitations as follows:

“The multi-word arithmetic device of Claim 6, wherein the control circuit determines whether a carry has been generated by the arithmetic unit immediately after completion of the processing (1) to (3) and if a carry has been generated, further controls the memory input/output circuit and the adder to execute the following processing:

Art Unit: 2137

(4) the memory input/output circuit (a) reads simultaneously, from the integers W and P stored in the memory, pieces of one-word data w and p, each with a same digit position, and has the read pieces of data input into the arithmetic unit, while (b) storing in the memory a piece of one-word data c output from the arithmetic unit and repeats processes (a) and (b) sequentially from a lowest-order word in each integer until n words of data are obtained, enabling an n-word integer C to be stored in the memory; and

(5) the arithmetic unit repeats n times a process in which the pieces of data w and p received from the memory input/output circuit are computed as $w + p$, propagating a carry, and a result c is output.” see column 3, lines 26-33; column 3, lines 50-56; column 7, line 33 to column 8, line 20 and column 12, line 30 to column 13, line 20.

Regarding claim 8, Sabin meets the claimed limitations as follows:

“The multi-word arithmetic unit of Claim 1, wherein the at least two types of modular arithmetic include Montgomery reduction calculating a residue for $A \cdot R^{(-1)} \bmod P$, when each word has k bits, A is a $2n$ -word integer used for input data, R is an integer $2^{(k \cdot n)}$ and P is an n-word integer; and

upon receiving, from the external device, an instruction to execute Montgomery reduction and an indication of a number of words $2n$ for an integer A on which Montgomery reduction is to

be performed, the control circuit controls the memory input/output circuit and the arithmetic unit to execute Montgomery reduction.” see column 3, lines 26-33; column 3,

Art Unit: 2137

lines 50-56; column 7, line 33 to column 8, line 20; column 12, line 30 to column 13, line 20 and column 17, line 29 to column 21, line 37.

Regarding claim 9, Sabin meets the claimed limitations as follows:

"The multi-word arithmetic device of Claim 8, wherein, when receiving an instruction to execute Montgomery reduction from the external device, the control circuit controls the memory input/output circuit and the arithmetic unit so as to execute the following processing:

(1) the memory input/output circuit acquires integers A, P and V from the external device and stores the obtained integers in the memory, the integer V being $-P^{-1} \bmod R$;

(2) the arithmetic unit computes partial products for words from each of (i) a lower n words of the integer A stored in the memory, and (ii) the integer V, and accumulates words in partial products having a same digit position, repeating the process sequentially from a lowest word in each integer until n words of accumulated results are obtained, and storing the accumulated results in the memory as a piece of n-word intermediate data B;

(3) the arithmetic unit computes partial products for words from each of (a) the piece of intermediate data B and (b) the integer P stored in the memory, and accumulates words in the partial products having a same digit position so that, when a lowest word is a 0th word, accumulated results for a 0th to (n-3)th word are not obtained, but accumulated results for a (n-2)th word to a (2n-1)th word are obtained and stored in the memory as the upper (n+1) words of a piece of intermediate data D;

Art Unit: 2137

(4) the arithmetic unit (a) generates (i) a carry obtained from a one-word addition performed by adding a lowest word from each of the piece of intermediate data D and an integer AA, and (ii) a one-bit logical value, the integer AA being an upper (n+1) words of the integer A, and the one-bit logical value being 0 when a one-word addition result is 0, and 1 when the one-word addition result is not 0, and (b) adds an upper n words of the piece of intermediate data D, an upper n words of the integer AA, the carry and the one-bit logical value, by repeating addition of word units sequentially from a lowest word in each integer, while propagating a carry, until n words of data are obtained, and stores an addition result in the memory as a piece of n-word output data M; and

(5) when the output data M stored in the memory is at least as large as the integer P, the arithmetic unit subtracts the integer P from the output data M until the output data M is 0 or a positive integer smaller than the integer P, by repeating subtraction of word units sequentially from a lowest word in each integer, while propagating a carry, until n words of data are obtained, and stores the subtraction results in the memory as a new piece of n-word output data M." see column 3, lines 26-33; column 3, lines 50-56; column 7, line 33 to column 8, line 20; column 12, line 30 to column 13, line 20 and column 17, line 29 to column 21, line 37.

Regarding claim 10, Sabin meets the claimed limitations as follows:

"The multi-word arithmetic device of Claim 9, wherein in processing (4), the arithmetic unit adds a piece of one-word data containing all ones to the piece of intermediate data D and the integer AA, and stores an upper n words of an obtained addition result in the memory as the output data M." see column 3, lines 26-33; column 3, line 50 to column

Art Unit: 2137

4, line 47; column 7, line 33 to column 8, line 20; column 12, line 30 to column 13, line 20 and column 17, line 29 to column 21, line 37.

Regarding claim 11, Sabin meets the claimed limitations as follows:

"The multi-word arithmetic device of Claim 10, wherein, in processing (2) and (3), the arithmetic unit selects sets of word pairs, each set formed from all the pairs of words that generate a partial product with a same digit position, sets input values in the multiplier, and computes and accumulates the partial products for the selected pairs of words in sequence from the set with a lowest digit position." see column 3, lines 26-33; column 3, line 50 to column 4, line 47; column 7, line 33 to column 8, line 20; column 12, line 30 to column 13, line 20 and column 17, line 29 to column 21, line 37.

Regarding claim 12, Sabin meets the claimed limitations as follows:

"The multi-word arithmetic device of Claim 11, wherein, in processing (2) and (3), the arithmetic unit stores in the memory as part of a multiplication result a lower word from a two-word accumulated result obtained by accumulating partial products with the same digit position, and adds an upper word from the accumulated result to partial products that have a digit position one word higher and are thus the next to be calculated." see column 3, lines 26-33; column 3, line 50 to column 4, line 47; column 7, line 33 to column 8, line 20; column 12, line 30 to column 13, line 20 and column 17, line 29 to column 21, line 37.

Regarding claim 13, Sabin meets the claimed limitations as follows:

"The multi-word arithmetic device of Claim 12, wherein the arithmetic unit performs an operation for storing a lower word from the accumulated result in the memory

Art Unit: 2137

simultaneously with an operation for adding an upper word from the accumulated result to partial products that have a digit position one word higher and are thus the next to be calculated.” see column 3, lines 26-33; column 3, line 50 to column 4, line 47; column 7, line 33 to column 8, line 20; column 12, line 30 to column 13, line 20 and column 17, line 29 to column 21, line 37.

Regarding claim 14, Sabin meets the claimed limitations as follows:

“The multi-word arithmetic device of Claim 10, wherein, when computing and accumulating partial products in processing (2) and (3), the arithmetic unit updates accumulated values by (a) simultaneously (i) computing a partial product and (ii) reading a previously accumulated one-word value from the memory, (b) adding the accumulated one-word value to a corresponding word in the partial product, and (c) storing a result of the addition in a corresponding area of the memory.” see column 3, lines 26-33; column 3, line 50 to column 4, line 47; column 7, line 33 to column 8, line 20; column 12, line 30 to column 13, line 20 and column 17, line 29 to column 21, line 37.

Regarding claim 15, Sabin meets the claimed limitations as follows:

“A multi-word arithmetic device for executing modular arithmetic on multi-word integers, in accordance with instructions from an external device, the multi-word arithmetic device comprising:

a memory;

an arithmetic unit for executing, on word units, at least two types of calculation, including addition and multiplication, and outputting a one-word calculation result; a

Art Unit: 2137

memory input/output circuit for performing (1) a first data transfer for storing in the memory at least one integer received from an external device, (2) a second data transfer for inputting at least one integer stored in the memory into the arithmetic unit in word units, (3) a third data transfer for storing in the memory the calculation result output from the arithmetic unit, and (4) a fourth data transfer for outputting the calculation result from the memory to the external device;

and a control circuit for, according to instructions received from the external device,

(a) specifying, to the memory input/output unit, data to be transferred by the second and third data transfers, and

(b) specifying, to the arithmetic unit, a type of calculation to be executed, thereby controlling:

(i) the arithmetic unit to selectively perform one of at least two types of modular arithmetic on the at least one integer stored in the memory; and

(ii) the memory input/output circuit to store the calculation result of the modular arithmetic into the memory, wherein the at least two types of modular arithmetic include modular addition and Montgomery reduction; and

the control circuit controls the memory input/output circuit and the arithmetic unit so that the arithmetic unit (1) computes $A+B \bmod P$ when an instruction for executing modular addition is received from the external device, A , B and P being n -word integers, and (2) computes a residue for $A \cdot R^{(-1)} \bmod P$, when an instruction for executing Montgomery reduction is received from the external device, each word having k bits, A being a

Art Unit: 2137

2n-word integer used as input data, R being an integer $2^{(k*n)}$ and P being an n-word integer.” see column 3, lines 26-33; column 3, line 50 to column 4, line 47; column 7, line 33 to column 8, line 20; column 11, lines 42-49; column 12, line 30 to column 13, line 20; column 17, line 29 to column 21, line 37 and column 17, line 29 to column 21, line 37.

Regarding claim 16, Sabin meets the claimed limitations as follows:

“The multi-word arithmetic unit of Claim 15, wherein the arithmetic unit includes:

a multiplier receiving an input of two pieces of one-word data and outputting a piece of two-word data;

an adder receiving an input of at least two pieces of two-word data, including a piece of two-word data output from the multiplier, and outputting a piece of multi-word data; and

a selecting circuit selecting, according to instructions from the control circuit:

(1), data to be input into one of the multiplier and the adder out of data transmitted from the memory input/output circuit; and

(2) data to be output as the calculation result out of data output from one of the adder and the multiplier.” see column 3, lines 26-33; column 3, line 50 to column 4, line 47; column 7, line 33 to column 8, line 20; column 11, lines 42-49; column 12, line 30 to column 13, line 20; column 17, line 29 to column 21, line 37 and column 17, line 29 to column 21, line 37.

Regarding claim 17, Sabin meets the claimed limitations as follows:

Art Unit: 2137

"The multi-word arithmetic unit of Claim 16, wherein the memory is divided into two dual-port memories, each allowing access to two storage areas designated by two addresses, and allowing (1) two read operations, or (2) one read operation and one write operation to be performed simultaneously on word units; and the at least two integers are stored in each dual-port memory so that the memory input/output circuit can simultaneously (1) read a piece of one-word data simultaneously from each of the integers stored in the two dual-port memories, and have the read pieces of data input into one of the adder and the multiplier, and (2) write a piece of one-word data output from one of the adder and the multiplier into one of the two dual-port memories." see column 3, lines 26-33; column 3, line 50 to column 4, line 47; column 7, line 33 to column 8, line 20; column 11, lines 42-49; column 12, line 30 to column 13, line 20; column 14, lines 28-53; column 17, line 29 to column 21, line 37 and column 17, line 29 to column 21, line 37.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Kessels (5,414,651) discloses an arithmetic unit used in a public key cryptosystem for multiplying long integers.

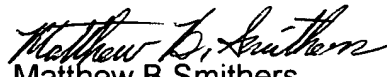
B. Lambert et al (6,049,815) discloses an apparatus for performing modular arithmetic over a set field of integers.

C. Paar et al (6,252,959) discloses a system for calculating points in an elliptic curve cryptosystem.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Matthew B Smithers
Primary Examiner
Art Unit 2137